UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI

WILLIAM COTON, JENNIFER BUTLER, and TRAVIS BUTLER individually and on behalf of all others similarly situated, Plaintiffs, v. ASCENSION HEALTH, a Missouri nonprofit corporation Defendant.	Cause No.: 4:25-CV-00072 CLASS ACTION COMPLAINT DEMAND FOR JURY TRIAL

CLASS ACTION COMPLAINT

1. Plaintiffs William Coton, Jennifer Butler and Travis Butler ("Plaintiffs") individually and on behalf of all others similarly situated, bring this action against Defendant Ascension Health ("Ascension" or "Defendant"), based upon personal knowledge as to themselves and their own acts, and as to all other matters upon information and belief, based upon, *inter alia*, the investigations of their attorneys.

NATURE OF THE ACTION

2. On or around May 7 or May 8, 2024, Ascension had its data servers breached by unauthorized third-party hackers, who stole the highly sensitive personal and medical information of approximately 5,599,999 individuals across the country. The stolen information included the individuals' medical information (such as medical record number, date of service, types of lab tests, or procedure codes), payment information (such as credit card information or bank account number), insurance information (such as Medicaid/Medicare ID, policy number, or insurance claim), government identification (such as Social Security number, tax identification number,

driver's license number, or passport number), and other personal information (such as date of birth or address).

3. Ascension is "one of the nation's leading non-profit and Catholic health systems," operating "across 17 states and the District of Columbia" and "encompassing approximately 128,000 associates, 33,000 affiliated providers, 118 wholly owned or consolidated hospitals, and 34 senior living facilities."[1] As a result, Ascension collects and stores the personal identifying information ("PII") and protected health information ("PHI") of millions of patients from across the country.

4. Under statute and regulation, Ascension had a duty to implement reasonable, adequate industry-standard data security policies safeguards to protect patient PII and PHI. Ascension recognizes and acknowledges these duties in the various "HIPAA Notice of Privacy Practices" posted on its website. For instance, Ascension's "Joint Notice of Privacy Practices" for the District of Columbia acknowledges that "[w]e are required by law to maintain the privacy and security of your health information," that "[w]e are committed to maintaining the privacy and confidentiality of your health information," and that "[w]e will not share your information other than as described here unless you tell us we can in writing."[2]

---

[1] https://about.ascension.org/about-us?_gl=1*vmuys6*FPAU*MTYyODEzNDE0Mi4xNzM1ODU0NTc1*_ga*MTk5NDgxMTEzMS4xNzM1ODU0NTg0*_ga_BGPJM8XFJ4*MTczNjM2MTk1MS4xLjAuMTczNjM2MTk1MS4wLjAuOTg4NjkzMjU1*_fplc*RzliS1dnVGNmYWRERUpEeFJxeHExRU5pUmpMWEVTZko0WDNGTVlkUGZMU20yMnIxeU1lWTlzMGZvcnRtU1VJc0ZLNCUyQkVSRkRGcXBZclI0cmdMMXdhN3RVJTJCVTN2TEFZRmVZZzJTeEhkT0RJYm5mc0pSU2l5ck1HaHJ1eUlBQSUzRCUzRA.

[2] chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://healthcare.ascension.org/-/media/healthcare/npp/washington-dc/dc_providence-health-system_english.pdf.

5. However, Ascension breached these assurances and promises to its patients that their PII and PHI would be secure by failing to implement reasonable and adequate safeguards, thereby failing to protect its patients' sensitive PII and PHI.

6. Plaintiffs, individually and on behalf of those similarly situated persons (hereafter "Class Members"), bring this Class Action to secure redress against Ascension for its reckless and negligent violation of their privacy rights. Plaintiffs and Class Members are patients and former patients of Ascension who had their PII and PHI collected, stored and ultimately breached by Ascension.

7. Plaintiffs protect their PII and PHI, understanding that disclosure of such sensitive information can wreak havoc when in the hands of nefarious persons. Thus, Plaintiffs ensure that all disclosures of their PII and PHI are only to the extent necessary. To receive medical services from Ascension, Ascension required Plaintiffs and Class Members' PII and PHI. Plaintiffs and Class Members relied on Ascension's assurances and promises that it would secure the PII and PHI in its possession with adequate safeguards knowing that medical treatment centers were often the targets of cybercriminals. It was foreseeable that, as a medical center that stores large swaths of sensitive patient PII and PHI, Ascension would inevitably be a target for a data breach. Despite this knowledge, Ascension failed to implement proper and adequate data security policies and systems it promised to Plaintiffs and Class Members. Plaintiffs and Class Members suffered injuries and damages and will continue to suffer injuries and damages, particularly given Ascension's unreasonable delay in notifying affected individuals. As a result of Ascension's wrongful actions and inactions, Plaintiffs' and Class Members' sensitive PII and PHI were compromised. Plaintiffs' and Class Members' privacy rights were violated, and they are now exposed to a heightened risk of identity theft and credit fraud for the remainder of their lifetimes.

Plaintiffs and Class Members must now spend time and money on prophylactic measures, such as increased monitoring of their personal and financial accounts and the purchase of credit monitoring services, to protect themselves from future loss. Plaintiffs and Class Members have also lost the value of their PII and PHI. Plaintiffs and Class Members would not have paid for Ascension's services or would not have paid as much as they did, had they known that Ascension did not intend to protect the PII and PHI in its possession, and thus, Plaintiffs and Class Members have lost the benefit of their bargains.

8. As a result of Ascension's wrongful actions and inactions, patient information was stolen. Plaintiffs and Class Members who have had their PII and PHI compromised by nefarious third-party hackers, have had their privacy rights violated, have been exposed to the risk of fraud and identity theft, and have suffered damages. Plaintiffs and Class Members bring this action to secure redress against Ascension.

THE PARTIES

9. Plaintiff William Coton is a citizen of the District of Columbia and a patient of an Ascension provider. On or around December 19, 2024, Mr. Coton received a data breach notice from Ascension informing him that his PII and PHI—including, *inter alia*, his medical information (such as medical record number, date of service, types of lab tests, or procedure codes), payment information (such as credit card information or bank account number), insurance information (such as Medicaid/Medicare ID, policy number, or insurance claim), government identification (such as Social Security number, tax identification number, driver's license number, or passport number), and other personal information (such as date of birth or address)—which he had entrusted for safekeeping with Ascension, had been breached in May 2024.

10. Plaintiff Jennifer Butler is a citizen of the District of Columbia and a patient of an Ascension provider. On or around December 19, 2024, Ms. Butler received a data breach notice from Ascension informing her that her PII and PHI—including, *inter alia*, her medical information (such as medical record number, date of service, types of lab tests, or procedure codes), payment information (such as credit card information or bank account number), insurance information (such as Medicaid/Medicare ID, policy number, or insurance claim), government identification (such as Social Security number, tax identification number, driver's license number, or passport number), and other personal information (such as date of birth or address)—which she had entrusted for safekeeping with Ascension, had been breached in May 2024.

11. Plaintiff Travis Butler is a citizen of the District of Columbia and a patient of an Ascension provider. On or around December 19, 2024, Mr. Butler received a data breach notice from Ascension informing him that his PII and PHI—including, *inter alia*, his medical information (such as medical record number, date of service, types of lab tests, or procedure codes), payment information (such as credit card information or bank account number), insurance information (such as Medicaid/Medicare ID, policy number, or insurance claim), government identification (such as Social Security number, tax identification number, driver's license number, or passport number), and other personal information (such as date of birth or address)—which he had entrusted for safekeeping with Ascension, had been breached in May 2024.

12. Since the data breach, Plaintiffs have spent increased time and money monitoring his personal and financial accounts for fraud, including, *inter alia*, an uptick of scam calls and messages and reports of fraudulent financial activity done in their names. In response, Mr. Coton has purchased a credit monitoring service to help him monitor his personal and financial accounts.

Had Plaintiffs known that Ascension would not protect their PII and PHI, they would not have purchased its services or only would have been willing to pay substantially less for them.

13. Ascension is a Missouri nonprofit corporation with its principal addresses located at 4600 Edmundson Road, Saint Louis, Missouri 63134-3806. Its agent for service of process is CSC Corporation, which can be served at 221 Bolivar Street, Jefferson City, Missouri 65101.

JURISDICTION AND VENUE

14. This Court has federal question subject matter jurisdiction pursuant to 28 U.S.C. § 1331 for claims that arise under the Stored Communications Act, 18 U.S.C. § 2701, *et seq*. The Court has supplemental jurisdiction under 28 U.S.C. § 1367 over the state claims because they are so related to the federal claims in that they form a part of the same case or controversy.

15. Additionally, this Court has subject matter jurisdiction over the state law claims asserted herein pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), as the amount in controversy in this action exceeds $5 million, there are putative Class Members, including Plaintiffs, that are domiciled in a different state than Ascension, and there are more than 100 putative Class Members.

16. The Court also has personal jurisdiction over Ascension because it routinely conducts business in this District and has sufficient minimum contacts in this District have intentionally availed itself to this jurisdiction by marketing and providing healthcare services in this District.

17. Venue is proper in this District because, among other things: (a) Ascension is incorporated in, headquartered in, and directed its activities at residents in this District; and (b) many of the acts and omissions that give rise to this action took place in this judicial District for services provided in this District.

18. Venue is further appropriate in this District pursuant to 28 U.S.C. § 1391 because, among other things: (a) Ascension's principal place of business is this District and it conducts substantial business in this District; (c) Ascension directed its services at residents in this District; and (d) many of the acts and omissions that give rise to this Action took place in this District.

FACTUAL ALLEGATIONS

A. The Data Breach

19. Ascension is a nationwide health network offering access to a wide variety of hospital and medical services. In order to obtain these services, Ascension requires that all patients provide their PII and PHI as a requirement to receive healthcare services from Ascension. As a result, Ascension's systems store the PII and PHI of millions of patients who have received its healthcare services.

20. On or around May 7 or May 8, 2024, Ascension 's systems were accessed by unauthorized third-party hackers, who exfiltrated Plaintiffs' and Class Members' sensitive PII and PHI—including, *inter alia*, medical information (such as medical record number, date of service, types of lab tests, or procedure codes), payment information (such as credit card information or bank account number), insurance information (such as Medicaid/Medicare ID, policy number, or insurance claim), government identification (such as Social Security number, tax identification number, driver's license number, or passport number), and other personal information (such as date of birth or address). In its data breach notification filed the Office of Maine Attorney General, Ascension reported that the data breach had affected 5,599,699 individuals.[3]

[3] https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/e55264f2-ff87-4b28-874d-653cfb735fe6.html.

B. Ascension's Duty to Protect Patient PII/PHI and Notify Patients Under State and Federal Law

21. Ascension, as a healthcare provider, holds a statutory duty under the Health Insurance Portability and Accountability Act ("HIPAA") to safeguard Plaintiffs' and Class Members' PII/PHI.

22. Under the HIPAA Privacy Rule, Ascension is required to:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives maintains or transmits;
b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and
d. Ensure compliance by their workforce.

45 C.F.R. § 164.306(a).

23. The HIPAA Privacy Rule also requires Ascension to "review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information" under 45 C.F.R. § 164.306(e) and to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights" under 45 C.F.R. § 164.312(a)(1).

24. Further, the Federal Trade Commission Act, 15 U.S.C. § 45 prohibits Ascension from engaging in "unfair or deceptive acts or practices affecting commerce." The Federal Trade Commission has found that a company's failure to maintain reasonable and appropriate data security for the consumers' sensitive personal information is an "unfair practice" in violation of the Federal Trade Commission Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 243 (3rd Cir. 2015).

25. Ascension failed to comply with each of these state and federal statutes by failing to implement and maintain reasonable security procedures to protect Plaintiffs' and Class Members' PII/PHI. As a result, Plaintiffs' and Class Members' sensitive PII/PHI was accessed and exfiltrated by nefarious third-party hackers.

26. Additionally, both HIPAA and Missouri state law required Ascension to timely notify Plaintiffs and Class Members of the data breach. Under HIPAA, Ascension is required to notify individuals affected by a data breach "without reasonable delay" or within 60 calendar days following the date of discovery of the data breach. 45 C.F.R. § 164.404. Likewise, Mo. Rev. Stat § 407.1500 required Ascension to notify consumers affected by a data breach "without unreasonable delay." Despite discovering the data breach on May 7 or May 8, 2024, Ascension did not provide the required data breach notices to Plaintiffs and Class Members until on or around December 19, 2024—over *seven* months later.

C. Applicable Standards of Care

27. In addition to its obligations under federal law, Ascension owed a duty to Plaintiffs and the Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the PII in their possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Ascension owed a duty to Plaintiffs and the Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that their computer system and networks, and the personnel responsible for them, adequately protected the PII/PHI of Plaintiffs and Class Members. Plaintiffs and Class Members entered into a special relationship with Ascension, beyond a mere customer-retailer relationship, as Ascension provided medical health services that, by their nature, require the utmost care, discretion, and confidentiality to effectuate effective services.

28. Ascension owed a duty to Plaintiffs and the Class Members to design, maintain, and test its computer systems to ensure that the PII/PHI in its possession was adequately secured and protected. As it was foreseeable and there was a significant likelihood that, as provider requiring PII and PHI, Ascension would be a target for cybercriminals to seek unauthorized access to PII/PHI stored by Ascension.

29. Ascension owed a duty to Plaintiffs and the Class Members to create and implement reasonable data security practices and procedures to protect the PII/PHI in its possession, including adequately training its employees and others who accessed the PII/PHI in its possession, including adequately training its employees and others who accessed PII/PHI in its computer systems on how to adequately protect PII/PHI.

30. Ascension owed a duty of care to Plaintiffs and Class Members to implement processes that would detect a breach of its data security systems in a timely manner.

31. Ascension owed a duty to Plaintiffs and the Class Members to act upon data security warnings and alerts in a timely fashion.

32. Ascension owed a duty to Plaintiffs and Class Members to disclose if its computer systems and data security practices were inadequate to safeguard PII/PHI from theft because such an inadequacy would be a material fact for Plaintiffs and Class Members when deciding whether to provide or entrust their PII/PHI to Ascension.

33. Ascension owed a duty to Plaintiffs and the Class Members to disclose in a timely and accurate manner when the data breach occurred.

34. Ascension owed a duty of care to Plaintiffs and the Class Members because they were foreseeable and probable victims of any inadequate data security practices. Ascension received PII/PHI from Plaintiffs and Class Members with the understanding that Plaintiffs and

Class Members expected their PHI/PII to be protected from disclosure, as per Ascension's promises and assurances. Ascension knew that a breach of its data systems would cause Plaintiffs and Class Members to incur damages.

35. Ascension recognized and acknowledged these duties in its various "HIPAA Notice of Privacy Practices" posted on its website. For instance, Ascension's "Joint Notice of Privacy Practices" for the District of Columbia acknowledges that "[w]e are required by law to maintain the privacy and security of your health information," that "[w]e are committed to maintaining the privacy and confidentiality of your health information," and that "[w]e will not share your information other than as described here unless you tell us we can in writing."[4]

D. Stolen Information Is Valuable to Hackers and Thieves

36. It is well known, and the subject of many media reports, that PII/PHI is highly coveted and a frequent target of hackers. Especially in the technology industry, the issue of data security and threats thereto is well known. Despite well-publicized litigation and frequent public announcements of data breaches, including of providers of medical services, Ascension opted to maintain an insufficient and inadequate system to protect the PII/PHI of Plaintiffs and Class Members, despite its assurances and promises to safeguard the PII/PHI in Ascension's possession.

37. Plaintiffs and Class Members value their PII/PHI, as in today's electronic-centric world, their PII/PHI is required for numerous activities, such as new registrations to websites, or opening a new bank account, as well as signing up for special deals. Moreover, the frequency of fraudulent charges and identity theft cautioned Plaintiffs and Class Members to be even more

[4] chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://healthcare.ascension.org/-/media/healthcare/npp/washington-dc/dc_providence-health-system_english.pdf.

discerning as to the recipients of their PII/PHI. Plaintiffs and Class Members protect their PII/PHI and consider whether any recipient of PII/PHI would also similarly guard their PII/PHI.

38. Legitimate organizations and the criminal underground alike recognize the value of PII/PHI. That is why they aggressively seek and pay for it.

39. PII/PHI is highly valuable to hackers. Identity thieves use stolen PII/PHI for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud. PII/PHI that is stolen from the point of sale are known as "dumps."[5]

40. Once someone buys PII/PHI, it is then used to gain access to different areas of the victim's digital life, including bank accounts, social media, and credit card details. During that process, other sensitive data may be harvested from the victim's accounts, as well as from those belonging to family, friends, and colleagues.

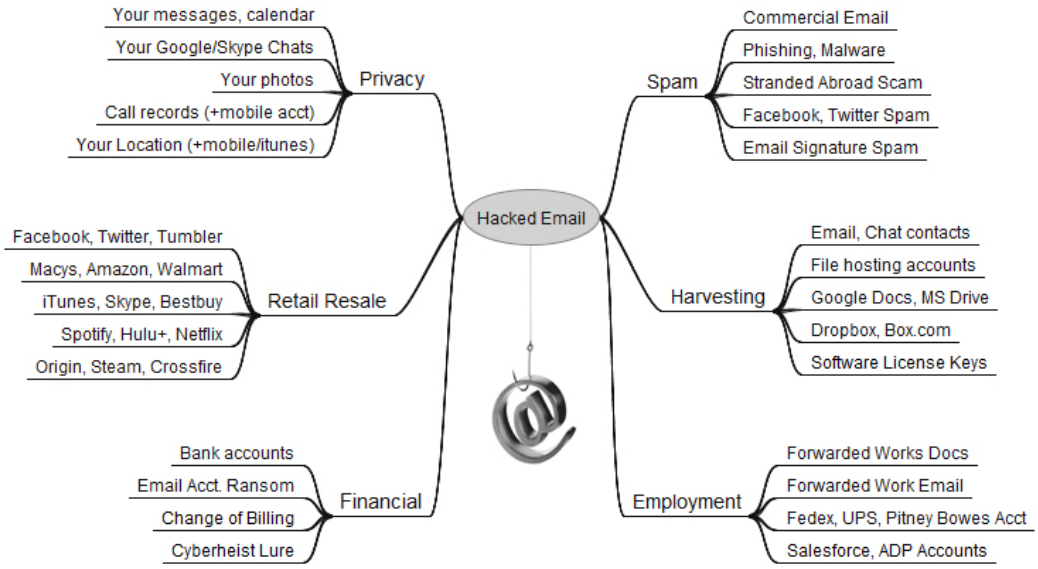
41. In addition to PII/PHI, a hacked email account can be very valuable to cybercriminals. Since most online accounts require an email address not only as a username, but also to verify accounts and reset passwords, a hacked email account could open up a number of other accounts to an attacker.[6]

---

[5] https://krebsonsecurity.com/2016/04/all-about-fraud-how-crooks-get-the-cvv/.

[6] https://www.trendmicro.com/vinfo/us/security/news/online-privacy/identity-theft-and-the-value-of-your-personal-data.

42. As shown below, a hacked email account can be used to link to many other sources of information for an identity thief, including any purchase or account information found in the hacked email account.[7]



43. Hacked information can also enable thieves to obtain other personal information through "phishing." According to the Report on Phishing available on the United States, Department of Justice's website: "AT&T, a large telecommunications company, had its sales system hacked into, resulting in stolen order information including full names and home addresses, order numbers and credit card numbers. The hackers then sent each customer a highly personalized e-mail indicating that there had been a problem processing their order and re-directing them to a spoofed website where they were prompted to enter further information, including birthdates and Social Security numbers."[8]

[7] https://krebsonsecurity.com/2013/06/the-value-of-a-hacked-email-account/.
[8] https://www.justice.gov/archive/opa/docs/report_on_phishing.pdf.

E. The Data Breach Has and Will Result in Additional Identity Theft and Fraud

44. Ascension failed to implement and maintain reasonable security procedures and practices appropriate to protect Plaintiffs' and the Class Members' PII/PHI. The ramification of Ascension's failure to keep Plaintiffs' and the Class Members' data secure is severe.

45. Between 2005 and 2019, at least 249 million individuals were affected by health care data breaches.[9] In 2019 alone, over 505 HIPAA data breaches were reported, resulting in over 41 million healthcare records being exposed, stolen, or unlawfully disclosed.[10] The frequency and severity of healthcare data breaches has only increased with time. 2021 was reported as the "worst ever year" for healthcare data breaches—with at least 44,993,618 healthcare records having been exposed or stolen across 585 breaches.[11] Thus, it was reasonably likely and foreseeable that Ascension would be a target given its possession of PII/PHI such that Ascension should have implemented better and stronger data security policies, procedures, and practices as it was only a matter of when, not if, cybercriminals would seek to infiltrate Ascension's systems to gain unauthorized access to PII/PHI.

46. It is incorrect to assume that reimbursing a consumer for a financial loss due to fraud makes that individual whole again. On the contrary, after conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that "among victims who had personal information used for fraudulent purposes, about a third (32%) spent a month or more resolving problems."[12] In fact, the BJS reported, "resolving the problems caused by identity theft [could] take more than a year for some victims." *Id*.

---

9 https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/.
10 https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/.
11 https://www.hipaajournal.com/largest-healthcare-data-breaches-of-2021/.
12 https://bjs.ojp.gov/content/pub/pdf/vit14.pdf.

F. Annual Monetary Losses from Identity Theft Are in the Billions of Dollars

47. Javelin Strategy and Research reports that losses from identity theft reached $21 billion in 2013. There may be a time lag between when harm occurs and when it is discovered, and between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches[13]:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

48. This is particularly the case with HIPAA data breaches such as Ascension's data breach, as the information implicated, such as Social Security numbers and medical history, cannot be changed. Once such information is breached, malicious actors can continue misusing the stolen information for years to come. Indeed, medical identity theft is one of the most common, most expensive, and most difficult-to-prevent forms of identity theft.[14] Victims of medical identity theft "often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[15]

49. Indeed, a study by Experian found that the average total cost of medical identity theft is "nearly $13,500" per incident, and that many victims were forced to pay out-of-pocket costs for fraudulent medical care.[16] Victims of healthcare data breaches often find themselves "being denied care, coverage or reimbursement by their medical insurers, having their policies

---

[13] http://www.gao. gov/new.items/d07737.pdf.
[14] https://khn.org/news/rise-of-indentity-theft/.
[15] *Id.*
[16] https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/.

canceled or having to pay to reinstate their insurance, along with suffering damage to their credit ratings and scores."[17]

50. Plaintiffs and the Class Members now face years of constant surveillance of their financial personal, and medical records, monitoring, and loss of rights. Plaintiffs and Class Members are incurring and will continue to incur such damages in addition to any financial or identity fraud they suffer.

G. Plaintiffs and Class Members Suffered Damages

51. The exposure of Plaintiffs' and Class Members' PII/PHI to unauthorized third-party hackers was a direct and proximate result of Ascension's failure to properly safeguard and protect Plaintiffs' and Class Members' PII from unauthorized access, use, and disclosure, as required by and state and federal law and as Ascension promised and assured Plaintiffs and Class Members it would. The data breach was also a result of Ascension's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiffs' and Class Members' PII/PHI to protect against reasonably foreseeable threats to the security or integrity of such information, also required by their contracts, promises, assurances, and state and federal law.

52. Plaintiffs' and Class Members' PII/PHI is private and sensitive in nature and was inadequately protected by Ascension. Ascension did not obtain Plaintiffs' and Class Members' consent to disclose their PII/PHI, except to certain persons not relevant to this action, as required by applicable law and industry standards.

53. As a direct and proximate result of Ascension's wrongful actions and inaction and the resulting data breach, Plaintiffs and Class Members have been placed at an imminent,

[17] *Id.*

immediate, and continuing risk of harm from identity theft and identity fraud, requiring them to take the time and effort to mitigate the actual and potential impact of the subject data breach on their lives by, among other things, paying for credit and identity monitoring services, spending time on credit and identity monitoring, placing "freezes" and "alerts" with credit reporting agencies, contacting their personal, financial and healthcare institutions, closing or modifying personal, financial or healthcare accounts, and closely reviewing and monitoring their credit reports, financial accounts and healthcare accounts for unauthorized activity.

54. Plaintiffs and Class Members also lost the value of their PII/PHI. PII/PHI is a valuable commodity, as evidenced by numerous companies that purchase PII from consumers, such as UBDI, which allows its users to link applications like Spotify, Twitter, or Apple Health and opt-in to paid opportunities to earn income, and Brave, which uses a similar business model, and by market-based pricing data involving the sale of stolen PII across multiple different illicit websites.

55. Top10VPN, a secure network provider, has compiled pricing information for stolen PII, including $160.15 for online banking details, $35.00 for credit reports, and $62.61 for passports. Standalone Yahoo! email accounts have been listed for as little as $0.41, while banking logins are in the range of $500, and verified PayPal accounts with high balances are listed at as much as $2,000.

56. In addition, Privacy Affairs, a cyber security research firm, has listed the following prices for stolen PII:

U.S. driving license, high quality:	$550
Auto insurance card:	$70
AAA emergency road service membership card:	$70
Wells Fargo bank statement:	$25
Wells Fargo bank statement with transactions:	$80
Rutgers State University student ID:	$70

57. Healthcare data is particularly valuable on the black market because it often contains all of an individual's PII and PHI, including information, such as a Social Security numbers or diagnosis and medical treatment information, that is not easily, or outright cannot be changed in response to a data breach. As a result, a healthcare data record may be valued at up to **$250 per record**.[18]

58. Ascension's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiffs' and Class Members' PII/PHI, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. The improper disclosure and theft of their PII/PHI;

b. The imminent and impending injury flowing from potential fraud and identity theft posed by their PII/PHI being exposed to and misused by unauthorized third-party hackers;

c. The untimely and inadequate notification of the data breach;

d. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the data breach; and

e. Ascertainable losses in the form of deprivation of the value of their PII/PHI, for which there is a well-established national and international market.

59. Finally, Plaintiffs and Class Members lost the benefit of their bargains. Plaintiffs and Class Members entered into agreements with and provided payment to Ascension under the

[18] "2018 Trustwave Global Security Report," TRUSTWAVE, https://trustwave.azureedge.net/media/15350/2018-trustwave-global-security-report-prt.pdf?rnd=131992184400000000 (last viewed Mar. 21, 2023).

reasonable but mistaken belief that Ascension would reasonably and adequately protect their PII/PHI. Plaintiffs and Class Members would not have entered into such agreements and would not have paid Ascension the amount that they paid had they known that Ascension would not reasonably and adequately protect their PII/PHI, as Ascension promised and assured Plaintiffs and Class Members it would. Plaintiffs and Class Members have thus suffered actual damages in an amount at least equal to the difference in value between the medical services that include reasonable and adequate data security that they bargained for, and the medical services that do not, which is what they actually received.

CLASS ACTION ALLEGATIONS

60. Plaintiffs bring this action on their own behalf and pursuant to the Federal Rule of Civil Procedure 23(a), (b)(2), (b)(3), and (c)(4). Plaintiffs intend to seek certification of the following class of affected individuals, initially defined as follows:

> All persons residing in the United States who received a data breach notice informing them that their PII/PHI had been breached by unauthorized third parties as a result of Ascension's data breach.

61. Excluded from the above Class definition is Ascension, including any entity in which Ascension has a controlling interest, is a parent or subsidiary, or which is controlled by Ascension, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Ascension. Also excluded are the judge and the court personnel in this case and any members of their immediate families. Plaintiffs reserve the right to amend the Class definitions if discovery and further investigation reveal that the Class should be expanded or otherwise modified.

62. *Numerosity*, Fed. R. Civ. P. 23(a)(1): The members of the Class are so numerous that the joinder of all members is impractical. The disposition of the claims of Class Members in

a single action will provide substantial benefits to all parties and to the Court. The Class Members are readily identifiable from information and records in Ascension's possession, custody, or control, such as treatment records and registrations

63. *Commonality*, Fed. R. Civ. P. 23(a)(2) and (b)(3): There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Ascension took reasonable steps and measures to safeguard Plaintiffs' and Class Members' PII and PHI;

b. Whether Ascension violated common and statutory by failing to implement reasonable security procedures and practices;

c. Which security procedures and which data-breach notification procedure should Ascension be required to implement as part of any injunctive relief ordered by the Court;

d. Whether Ascension knew or should have known of the security breach prior to the disclosure;

e. Whether Ascension has complied with any implied contractual obligation to use reasonable security measures;

f. Whether Ascension's acts and omissions described herein give rise to a claim of negligence;

g. Whether Ascension knew or should have known of the security breach prior to its disclosure;

h. Whether Ascension had a duty to promptly notify Plaintiffs and Class Members that their PII/PHI was, or potentially could be, compromised;

i. What security measures, if any, must be implemented by ASCENSION to comply with its duties under state and federal law;

j. The nature of the relief, including equitable relief, to which Plaintiffs and the Class Members are entitled; and

k. Whether Plaintiffs and the Class Members are entitled to damages, civil penalties, and/or injunctive relief.

64. *Typicality*. Fed. R. Civ. P. 23(a)(3): Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' PHI/PII, like that of every other Class Member, was misused and/or disclosed by Ascension.

65. *Adequacy of Representation*, Fed. R. Civ. P. 23(a)(4): Plaintiffs will fairly and adequately represent and protect Class Members' interests. Plaintiffs have retained competent counsel experienced in litigation of class actions, including consumer and data breach class actions, and Plaintiffs intend to prosecute this action vigorously. Plaintiffs' claims are typical of the claims of other Class Members and Plaintiffs have the same non-conflicting interests as the other Class Members. Therefore, the interests of the Class will be fairly and adequately represented by Plaintiffs and their counsel.

66. *Superiority of Class Action*, Fed. R. Civ. P. 23(b)(3): A class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all Class Members is impracticable. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

67. Damages for any individual Class Member are likely insufficient to justify the cost of individual litigation so that, in the absence of class treatment, Ascension's violations of law inflicting substantial damages in the aggregate would go un-remedied.

68. Class certification is also appropriate under Rule 23(a) and (b)(2), because Ascension has acted or refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

CAUSES OF ACTION

FIRST CAUSE OF ACTION

Violation of the Stored Communications Act, 18 U.S.C. § 2701, *et seq.*

69. Plaintiffs repeat and incorporate herein by reference each and every allegation contained in paragraphs 1 through 68, inclusive, of this Complaint as if set forth fully herein.

70. The Stored Communications Act ("SCA"), 18 U.S.C. § 2701, *et seq.* provides consumers with redress if a company mishandles their electronically stored information, such as PHI/PII. The SCA was designed, in part, to protect individuals' privacy interests in personal and proprietary information.

71. Section 2702(a)(1) of the SCA states that "a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service." 18 U.S.C. § 2702(a)(1).

72. "Electronic communication service" is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15).

73. Through its computer equipment, Ascension provides an "electronic communication service to the public" within the meaning of the SCA.

74. By failing to take reasonable steps to safeguard Plaintiffs' and Class Members' PHI/PII while in electronic storage, Ascension has allowed unauthorized access to its electronic systems and knowingly divulged patient PHI/PII.

75. Section 2702(a)(2)(A) of the SCA provides that "a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service on behalf of, and received by means of electronic transmission from (or created by means of computer processing or communications received by means of electronic transmission from), a subscriber or customer of such service." 18 U.S.C. § 2702(a)(2)(A).

76. "Remote computing service" is defined as "the provision to the public of computer storage or processing services by means of an electronic communications system." 18 U.S.C. § 2711(2).

77. "Electronic communications system" is defined as "any wire, radio, electromagnetic, photo-optical or photo electronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications." 18 U.S.C § 2510(14).

78. Ascension stores its patients' PHI/PII and utilizes such information to provide services to its patients.

79. By failing to take reasonable steps to safeguard PHI/PII and allowing its computer systems to be breached, Ascension knowingly divulged Plaintiffs' and Class Members' PHI/PII, and which allowed unauthorized persons to access and use the PHI/PII for improper purposes.

80. Upon learning that its systems had been intruded upon and information had been obtained and accessed by unauthorized third parties, Ascension failed to promptly inform Plaintiffs and Class Members of the data breach and continued to knowingly divulge PHI/PII to third parties.

81. Plaintiffs and Class Members have suffered actual injury and are entitled to damages in an amount to be proven at trial but in excess of the minimum jurisdictional requirement of this Court.

SECOND CAUSE OF ACTION

Negligence

82. Plaintiffs repeat and incorporate herein by reference each and every allegation contained in paragraphs 1 through 81, inclusive, of this Complaint as if set forth fully herein.

83. Ascension requires any individual that uses its services to provide their PII and PHI to Ascension. Ascension collects and stores this PII and PHI as a part of its regular business activities, and for its own pecuniary gain.

84. Ascension owed Plaintiffs and the Class Members a duty of care in the handling of its patient's PII. This duty included, but was not limited to, keeping PII/PHI secure and preventing disclosure to any unauthorized third parties. This duty of care existed independently of ASCENSION'S contractual duties to Plaintiffs and the Class Members. Under the FTC Guidelines, and other sources of industry-wide cybersecurity standards, Ascension is obligated to incorporate adequate measures to safeguard and protect PII/PHI that is entrusted to it in its ordinary course of business and transactions with customers.

85. Pursuant to the Federal Trade Commission Act, 15 U. S. C. § 45, Ascension had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs and Class Members' PII/PHI. The FTC has brought enforcement actions against

businesses for failing to adequately and reasonably protect customer information, treating the businesses' failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45. Orders from these actions further clarify the measures businesses are required to undertake to satisfy their data security obligations.[19]

86. Additional industry guidelines which provide a standard of care can be found in NIST's *Framework for Improving Critical Infrastructure Cybersecurity*.[20] NIST's Framework identifies seven steps for establishing or improving a cybersecurity program (section 3. 2). Those steps are:

> *Step 1: Prioritize and Scope*. The organization identifies its business/mission objectives and high-level organizational priorities. With this information, the organization makes strategic decisions regarding cybersecurity implementations and determines the scope of systems and assets that support the selected business line or process. The Framework can be adapted to support the different business lines or processes within an organization, which may have different business needs and associated risk tolerance. Risk tolerances may be reflected in a target Implementation Tier.
>
> *Step 2: Orient*. Once the scope of the cybersecurity program has been determined for the business line or process, the organization identifies related systems and assets, regulatory requirements, and overall risk approach. The organization then consults sources to identify threats and vulnerabilities applicable to those systems and assets.
>
> *Step 3: Create a Current Profile*. The organization develops a Current Profile by indicating which Category and Subcategory outcomes from the Framework Core are currently being achieved. If an outcome is partially achieved, noting this fact will help support subsequent steps by providing baseline information.
>
> *Step 4: Conduct a Risk Assessment*. This assessment could be guided by the organization's overall risk management process or previous risk assessment activities. The organization analyzes the operational environment in order to discern the likelihood of a cybersecurity event and the impact that the event could

[19] https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement

[20] https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf

have on the organization. It is important that organizations identify emerging risks and use cyber threat information from internal and external sources to gain a better understanding of the likelihood and impact of cybersecurity events.

Step 5: Create a Target Profile. The organization creates a Target Profile that focuses on the assessment of the Framework Categories and Subcategories describing the organization's desired cybersecurity outcomes. Organizations also may develop their own additional Categories and Subcategories to account for unique organizational risks. The organization may also consider influences and requirements of external stakeholders such as sector entities, customers, and business partners when creating a Target Profile. The Target Profile should appropriately reflect criteria within the target Implementation Tier.

Step 6: Determine, Analyze, and Prioritize Gaps. The organization compares the Current Profile and the Target Profile to determine gaps. Next, it creates a prioritized action plan to address gaps – reflecting mission drivers, costs and benefits, and risks – to achieve the outcomes in the Target Profile. The organization then determines resources, including funding and workforce, necessary to address the gaps. Using Profiles in this manner encourages the organization to make informed decisions about cybersecurity activities, supports risk management, and enables the organization to perform cost-effective, targeted improvements.

Step 7: Implement Action Plan. The organization determines which actions to take to address the gaps, if any, identified in the previous step and then adjusts its current cybersecurity practices in order to achieve the Target Profile. For further guidance, the Framework identifies example Informative References regarding the Categories and Subcategories, but organizations should determine which standards, guidelines, and practices, including those that are sector specific, work best for their needs.

87. In addition to its obligations under state and federal regulations and industry standards, Ascension owed a duty to Plaintiffs and the Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII/PHI in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Ascension owed a duty to Plaintiffs and the Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems and networks, and the personnel responsible for them, adequately protected the PII/PHI of Plaintiffs and the Class Members.

88. Ascension owed a duty to Plaintiffs and the Class Members to design, maintain, and test its internal data systems to ensure that the PII/PHI in Ascension's possession was adequately secured and protected.

89. Ascension owed a duty to Plaintiffs and the Class Members to create and implement reasonable data security practices and procedures to protect the PII/PHI in its custodianship, including adequately training its employees and others who accessed PII/PHI within its computer systems on how to adequately protect PII/PHI.

90. Ascension owed a duty to Plaintiffs and the Class Members to implement processes or safeguards that would detect a breach of their data security systems in a timely manner.

91. Ascension owed a duty to Plaintiffs and the Class Members to act upon data security warnings and alerts in a timely fashion.

92. Ascension owed a duty to Plaintiffs and the Class Members to timely disclose if its computer systems and data security practices were inadequate to safeguard individuals' PII/PHI from theft because such an inadequacy would be a material consideration in Plaintiffs' and Class Members' decisions to entrust their PHI/PII to Ascension.

93. Ascension owed a duty to Plaintiffs and the Class Members to disclose in a timely and accurate manner when data breaches occur.

94. Ascension owed a duty of care to Plaintiffs and the Class Members because they were foreseeable and probable victims of any inadequate data security practices and systems. ASCENSION collected PII from Plaintiffs and the Class Members. Ascension knew that a breach of its data systems would cause Plaintiffs and the Class Members to incur damages.

95. Ascension breached its duties of care to safeguard and protect the PII/PHI entrusted to it by Plaintiffs and the Class Members. Upon information and belief, Ascension adopted

inadequate safeguards to protect the PII/PHI and failed to adopt industry-wide standards set forth above in its supposed protection of the PII/PHI. Ascension failed to design, maintain, and test its computer system to ensure that the PII/PHI was adequately secured and protected, failed to create and implement reasonable data security practices and procedures, failed to implement processes that would detect a breach of its data security systems in a timely manner, failed to disclose the breach to potentially affected customers in a timely and comprehensive manner, and otherwise breached each of the above duties of care by implementing careless security procedures which led directly to the breach.

96. Ascension breached the duties set forth in 15 U.S.C. § 45, the FTC guidelines, the NIST's Framework for Improving Critical Infrastructure Cybersecurity, and other industry guidelines. In violation of 15 U.S.C. § 45, Ascension failed to implement proper data security procedures to adequately and reasonably protect Plaintiffs' and Class Member's PII/PHI. In violation of the FTC guidelines, *inter alia*, Ascension did not protect the personal customer information that it keeps; failed to properly dispose of personal information that was no longer needed; failed to encrypt information stored on computer networks; lacked the requisite understanding of their network's vulnerabilities; and failed to implement policies to correct security problems. In violation of the NIST's Framework, Ascension, *inter alia*, failed to adopt sufficient resources to identity and address security gaps.

97. Ascension's failure to comply with applicable laws and regulations constitutes negligence per se.

98. As a direct and proximate result of Ascension's failure to adequately protect and safeguard the PII/PHI, Plaintiffs and the Class Members suffered damages. Plaintiffs and the Class Members were damaged because their PII/PHI was accessed by third parties, resulting in increased

risk of identity theft, property theft and extortion for which Plaintiffs and the Class Members were forced to adopt preventive and remedial efforts. These damages were magnified by the passage of time because Ascension failed to notify Plaintiffs and Class Members of the data breach until weeks had passed. In addition, Plaintiffs and Class Members were also damaged in that they must now spend copious amounts of time combing through their records to ensure that they do not become the victims of fraud and/or identity theft.

99. Plaintiffs and Class Members have suffered actual injury and are entitled to damages in an amount to be proven at trial but in excess of the minimum jurisdictional requirement of this Court.

THIRD CAUSE OF ACTION

Breach of Implied Contract

100. Plaintiffs repeat and incorporate herein by reference each and every allegation contained in paragraphs 1 through 99, inclusive, of this Complaint as if set forth fully herein.

101. Plaintiffs and Class Members entered into agreements for medical treatment with Ascension. In making those agreements, Ascension solicited and invited Plaintiffs and Class Members to provide their PII and PHI to Ascension as requirement of receiving service. Plaintiffs and Class Members accepted Ascension's offers and provided their PII and PHI to enter the agreements. Inherent within those agreements was an implied contractual obligation that Ascension would implement reasonable and adequate data security to safeguard and protect the PII and PHI entrusted to it by Plaintiffs and Class Members from unauthorized disclosure. Ascension promised and assured Plaintiffs and Class Members in its various "HIPAA Notice of Privacy Practices" posted on its website. For instance, Ascension's "Joint Notice of Privacy Practices" for the District of Columbia acknowledges that "[w]e are required by law to maintain

the privacy and security of your health information," that "[w]e are committed to maintaining the privacy and confidentiality of your health information," and that "[w]e will not share your information other than as described here unless you tell us we can in writing."[21]

102. Thus, there was mutual assent when Plaintiffs and Class Members provided their PII and PHI to Ascension in exchange for medical services, they entered into implied contracts with Ascension under which Ascension agreed to and was obligated to reasonably protect their PII and PHI. There was consideration when Plaintiffs and Class Members provided payment to Ascension, as well as their PII and PHI, under the reasonable belief that any money they paid to Ascension in connection to its provision of medical services would be used in part to provide reasonable and adequate data security for their PII and PHI.

103. This implied contract is acknowledged and memorialized in Ascension's customer-facing documents, including, *inter alia*, Ascension's online "Privacy Notice for Health Information Practices," which states: "[w]e will not use or disclose your health information without your authorization."[22]

104. Ascension did not provide reasonable and adequate data security for Plaintiffs' and Class Member's PII and PHI, and instead caused it to be disclosed to unauthorized third-party hackers. Ascension did not comply with federal statute and regulation and did not comply with industry data security standards. In doing so, Defendant materially breached its obligations under implied contract.

105. That Ascension would implement such reasonable and adequate data security was a material prerequisite to the agreements between Plaintiffs and Class Members on the one hand

---

[21] chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://healthcare.ascension.org/-/media/healthcare/npp/washington-dc/dc_providence-health-system_english.pdf.

[22] https://www.menaregional.com/wp-content/uploads/2016/07/MRHSNPPMAY2014.pdf.

and Ascension on the other. Reasonable consumers value the privacy of their PII and PHI, and do not enter into agreements for medical services with healthcare providers which are known not to protect customer data. Accordingly, Plaintiffs and Class Members would not have entered into agreements with Ascension and would not have provided it with their sensitive PII and PHI, had they known that Ascension would not implement such reasonable and adequate data security.

106. As a result of Ascension's breach, Plaintiffs and Class Members lost the benefit of their bargains. Plaintiffs and Class Members entered into agreements with Ascension under the reasonable belief that Ascension would reasonably and adequately protect their PII/PHI and would not have entered into such agreements had they known that Ascension would not reasonably and adequately protect their PII/PHI. Plaintiffs and Class Members have thus suffered actual damages in an amount at least equal to the difference in value between the medical services that include reasonable and adequate data security that they bargained for, and the medical services that do not that they actually received.

107. Plaintiffs and Class Members fully performed their obligations under the implied contract by providing their PII/PHI and making payments to Ascension.

108. Plaintiffs and Class Members have suffered actual injury and are entitled to damages in an amount to be proven at trial but in excess of the minimum jurisdictional requirement of this Court.

FOURTH CAUSE OF ACTION

Unjust Enrichment

109. Plaintiffs repeat and incorporate herein by reference each and every allegation contained in paragraphs 1 through 108, inclusive, of this Complaint as if set forth fully herein.

110. Plaintiffs and Class Members provided their PII and PHI and conferred a monetary

benefit upon Ascension in exchange for healthcare services and adequate security and protection of their PII/PHI. Plaintiffs and Class Members did so under the reasonable belief that a specific portion of their monetary payment to Ascension was for the implementation and maintenance of reasonable, adequate, and statutorily mandated safeguards to protect their PII and PHI. Ascension was enriched when it sold its healthcare services at a higher price than it otherwise would have based on those beliefs.

111. Ascension's enrichment came at the expense of Plaintiffs and Class Members, who provided payment to Ascension, as well as their sensitive PII and PHI, under the reasonable belief that any money they paid to Ascension in connection to its provision of medical services would be used in part to provide reasonable and adequate data security for their PII and PHI. Plaintiffs and Class Members would not have paid for Ascension's services, or would have only been willing to paid substantially less for them, had they been aware that Ascension had not implemented reasonable, adequate and statutorily mandated safeguards to protect their PII and PHI..

112. As a direct and proximate result of Ascension's wrongful actions and inactions, Plaintiffs and Class Members suffered damages in the form of their lost benefit of the bargains. Plaintiffs and Class Members entered into agreements with Ascension under the belief that it would reasonably and adequately protect their PII/PHI. Plaintiffs and Class Members would not have entered into such agreements had they known that Ascension would not reasonably and adequately protect their PII/PHI. Plaintiffs and Class Members have thus suffered actual damages in an amount at least equal to the difference in value between the medical services that include reasonable and adequate data security that they bargained for, and the medical services that do not that they actually received.

113. Ascension should not be permitted to retain Plaintiffs' and Class Member's lost

benefits, without having adequately implemented the data privacy and security procedures for itself that Plaintiffs and Class Members paid for and that were otherwise mandated by federal, state, and local laws. and industry standards. Ascension should not be allowed to benefit at the expense of consumers who trust Ascension to protect the PII and PHI that they are required to provide to Ascension to receive its services.

114. As a direct and proximate result of Ascension's fraudulent conduct, Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial but in excess of the minimum jurisdictional requirement of this Court.

FIFTH CAUSE OF ACTION

Breach of Fiduciary Duty

115. Plaintiffs repeat and incorporate herein by reference each and every allegation contained in paragraphs 1 through 114, inclusive, of this Complaint as if set forth fully herein.

116. Plaintiffs and Class Members provided their PII and PHI to Ascension in confidence and under the reasonable belief that Ascension would protect the confidentiality of that information. Plaintiffs and Class Members would not have provided Ascension with their PII and PHI had they known that Ascension would not take reasonable and adequate steps to protect it.

117. Ascension's acceptance and storage of Plaintiffs' and Class Members' PII and PHI created a fiduciary relationship between Ascension and Plaintiffs and Class Members. As a fiduciary of Plaintiffs and Class Members, Ascension has duty to act primarily for the benefit of its patients and health plan participants, which includes implementing reasonable, adequate, and statutorily complaint safeguards to protect Plaintiffs' and Class Members' PII and PHI.

118. Far apart from a normal commercial relationship, Plaintiffs and Class Members put special trust and confidence in their relationship with Ascension, a medical provider. Ascension,

as a medical provider, occupies a position of trust and confidence as regards its patients such that a special fiduciary relationship exists between Plaintiffs and Class Members and Ascension. Akin to a doctor-patient relationship, Plaintiffs and Class Members held Ascension is such high regard as to trust ASCENSION's assurances and promises as to the confidentiality, sensitivity, and security of their PII/PHI.

119. In addition, Ascension encourages this special relationship and the trust ingrained in it by making explicit its promises and assurances in its various "HIPAA Notice of Privacy Practices" posted on its website. For instance, Ascension's "Joint Notice of Privacy Practices" for the District of Columbia acknowledges that "[w]e are required by law to maintain the privacy and security of your health information," that "[w]e are committed to maintaining the privacy and confidentiality of your health information," and that "[w]e will not share your information other than as described here unless you tell us we can in writing."[23]

120. Ascension breached its fiduciary duties to Plaintiffs and Class Members by, *inter alia,* failing to implement reasonable and adequate data security protections, failing to comply with the data security guidelines set forth by the FTC, NIST and HIPAA, failing to implement reasonable and adequate data security training for its employees, and otherwise failing to reasonably and adequately safeguard the PII and PHI of Plaintiffs and Class Members.

121. As a direct and proximate result of Ascension's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered damages. Plaintiffs and the Class Members were damaged because their PII/PHI was accessed by third parties, resulting in increased risk of identity theft, property theft and extortion for which Plaintiffs and the Class Members were forced to adopt

[23] chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://healthcare.ascension.org/-/media/healthcare/npp/washington-dc/dc_providence-health-system_english.pdf.

preventive and remedial efforts. These damages were magnified by the passage of time because Ascension failed to notify Plaintiffs and Class Members of the data breach until nearly six months after the data breach had been discovered. In addition, Plaintiffs and Class Members were also damaged in that they must now spend copious amounts of time combing through their records to ensure that they do not become the victims of fraud and/or identity theft. Importantly, Plaintiffs and Class Members suffered damages in the form of their lost benefit of the bargains. Plaintiffs and Class Members entered into agreements with Ascension under the belief that it would reasonably and adequately protect their PII/PHI. Plaintiffs and Class Members would not have entered into such agreements had they known that Ascension would not reasonably and adequately protect their PII/PHI. Plaintiffs and Class Members have thus suffered actual damages in an amount at least equal to the difference in value between the medical services that include reasonable and adequate data security that they bargained for, and the medical services that do not that they actually received.

122. As a direct and proximate result of Ascension's fraudulent conduct, Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial but in excess of the minimum jurisdictional requirement of this Court.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all Class Members, respectfully request that the Court enter judgment in their favor and against Ascension as follows:

1. For an Order certifying the Class as defined herein and appointing Plaintiffs and their Counsel to represent the Class;
2. For equitable relief enjoining Ascension from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and

Class Members' PII and PHI, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiffs and Class Members;

3. For equitable relief compelling Ascension to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety and to disclose with specificity to Class Members the type of PII/PHI compromised.

4. For an award of actual damages, statutory damages and compensatory damages, in an amount to be determined at trial;

5. For an award of punitive and treble damages, in an amount to be determined at trial;

6. For an award of costs of suit, litigation expenses and attorneys' fees, as allowable by law; and

7. For such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs, on behalf of themselves and all others similarly situated, hereby demand a jury trial for all claims so triable.

Dated: January 16, 2025

Respectfully submitted,

By: /s/ Matthew J. Devoti

Matthew J. Devoti (MO Bar No. 47751)
Matthew C. Casey (MO Bar No. 49662)
CASEY DEVOTI & BROCKLAND
5100 Dagget Avenue
St. Louis, Missouri 63110
mdevoti@caseydevoti.com
mcasey@caseydevoti.com

Jesenia A. Martinez*
**pro hac vice* forthcoming
WILSHIRE LAW FIRM, PLC
3055 Wilshire Boulevard, 12th Floor
Los Angeles, CA 90010
T: (213) 381-9988
F: (213) 381-9989
E: thiago@wilshirelawfirm.com

Attorneys for Plaintiffs and the Putative Class